As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(03):120-124, 2022
Copyright © 2022 International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0803025
Available online at: http://www.ijmtst.com/vol8issue03.html

Cloud-based multi-keyword search for multiple owners of encrypted data

Mandala Lakshmi Venkata Avinash[1] | M.Rajakumar[2]

[1]PG Scholar, Department of CSE, Pragati Engineering College (Autonomous), Surampalem, Andhra Pradesh
[2]Associate Professor, Department of CSE, Pragati Engineering College (Autonomous), Surampalem, Andhra Pradesh
Corresponding Author Email ID: mlvavinash7@gmail.com

To Cite this Article
Mandala Lakshmi Venkata Avinash and M.Rajakumar. Cloud-based multi-keyword search for multiple owners of encrypted data. International Journal for Modern Trends in Science and Technology 2022, 8(03), pp. 120-124. https://doi.org/10.46501/IJMTST0803025

Article Info
Received: 08 February 2022; Accepted: 10 March 2022; Published: 16 March 2022.

ABSTRACT

In order to store their massive amounts of data, many people are turning to distributed storage. It isn't only individuals or small businesses that are making use of distributed storage; large corporations are as well. Since it is so simple to use, the number of people who are adopting distributed storage is steadily increasing more than likely, the data stored in the cloud contains some enigmatic documents. It's crucial to have a safe place to store and retrieve your data. A wide range of cloud-based computations are available. Fewer companies provide valid insurance coverage for data that is backed up. A tree-based multi-watchword search strategy may be used to broaden categorization on account of numerous information owners. The TF-IDF model is used to construct a multi-catchphrase search and return the most relevant query items by considering a large amount of cloud-based data. Cloud servers also use a depth-first search calculation to find the relevant content in the cloud.

KEYWORDS : TF-IDF,Distributed Storage, TBMSM, PRMSM

1. INTRODUCTION

As computerized information, data is stored in lawful pools as part of distributed storage. In a circumstance when there are many owners, the same information will be shared among them. The whole data will be stored on a single server. Each server in the cloud may be located in a different part of the world. The put-away information will be under the control of either the primary server or the distributed storage providers. Cloud customers will buy or rent storage space from these distributed storage providers. Dispersed storage enables a wide range of systems to access the digital data. The Verified quest through the encoded data is a challenge that has to be addressed in distributed storage. Verified search on encoded cloud information is the most challenging distributed storage project. There are a variety of hunting plans available. As a matter of fact, these strategies either need a large amount of framework overhead or are exceedingly difficult to implement across large informative indexes. The information will be stored in the cloud in a scrambled structure to prevent unauthenticated access. A tree-based multi-word search scheme is constructed in order to supply a proficient search. There are distinct terms that emerge as report watchwords and a record is formed. As a result, all the lists structured in this way become one. To identify the client's comparative information document for each search request, a depth first search is used. Top results are restored using the TF-IDF model. An successful inquiry is conducted via a depth-first search.

Using the associated watchwords, a customer may describe any mapping of words to those reports in case only records containing a certain set of terms are to be recovered. Clients should describe any mapping or method to distributed storage beforehand to ensure the greatest possible information recovery. It's essential that the method doesn't compromise the security of any personal information. In a cloud, a client may access and construct information over the internet. Anywhere in the world should be able to access this information. Having a proper backup and recovery system is essential since all of the work is done on the server. There are, however, certain security risks if the information hoarding has not been properly protected. If you try to use these strategies across big informative indices, the results will be tough to get, whether in terms of framework overhead or sometimes. The information will be stored in the cloud in a scrambled structure to prevent unauthenticated access. A tree-based multi-word search scheme is constructed in order to supply a proficient search. There are distinct terms that emerge as report watchwords and a record is formed. As a result, all the lists structured in this way become one. It is used to find out the client's comparative information document for each search request. Top results are restored using the TF-IDF model. An successful inquiry is conducted via a depth-first search. Using the associated watchwords, a customer may describe any mapping of words to those reports in case only records containing a certain set of terms are to be recovered. Clients should describe any mapping or method to distributed storage beforehand to ensure the greatest possible information recovery. It's essential that the method doesn't compromise the security of any personal information. In a cloud, a client may access and construct information over the internet. Anywhere in the world should be able to access this information. It is essential to have a proper backup and recovery system in place since all of the work is done on the server. In any event, there are certain security concerns if the information accumulating is not properly protected.

2. LITERATURE SURVEY

These days, the cloud server is being used for encrypted information enquiry. Cloud information encoded by Wang et al. [20] may be safeguarded by an inquiry plot. Customer data is encrypted and sent to the cloud server in a scrambled manner, allowing for watchword searches on the ciphertext. An invulnerable reappropriated information look may be achieved by use of accessible encryption (SE) procedures. It is less expensive to pursue cloud facts that have been jumbled since it is more secure. A cloud-based search engine is used for all of these searches: multi-word search, fuzzy catchphrase search, and comparison search. In order to deal with the problem of a multi-watchword search for several data suppliers and multiple data clients in a distributed computing environment, various-key scrambled catchphrases coordinating and safety safeguarding located search of file techniques are used. If there are many people who have access to the data, then the system becomes less flexible and more difficult to utilise. [3] and [9] are two examples. When aggressors pretending to be professional information customers undertake an inspection, the system is protected by the information client verification approach. Consumers acquire search skills below those of neighbourhood trusted pros using Ming Li's recommended approval system (LTAs). To authenticate cloud clients before accessing their data, outsiders (TPA) were deployed. An further defence against attackers is client disavowal, in which information consumers are unable to carry out any missions after he has been rejected. A single keyword search is often all that is provided by the earliest of works. Then a couple multi-word search strategies were presented. It is the responsibility of data owners to maintain their data scrambled while the information consumers are responsible for creating access points via which queries may be sent in an encoded format. The use of re-encryption of a watchword list and trapdoors to increase the level of protection against attackers As a result, Wenhai Sun presented a tree-based report structure, with the purpose of making available inquiry productivity evident. According to Ning Cao's proposal, it is possible to find a large number of matches based on the relevance of records documents to the query and the internal item comparability to quantitatively assess such proximity. For dynamic tasks like document erasure and archive inclusion, Zhihua Xia devised an image that uses a tree-based file structure. When searching for many catchphrases, the greedy Depth-first Search calculation was utilised. Confounded rationale search is supported by Hongwei Li, who uses the combined AND, OR and NO things to do of catchphrases for a functioning and very expert multi-watchword search strategy. search over scrambled cloud information using custom-made multi-watchword search terms Semantic metaphysics WordNet and the search history of individual customers are used to develop a customer intrigue model.

3.EXISTING SYSTEM

The capacity to exchange records of information is yet another essential service. Health care professionals and patients should have the ability to view each other's top-k documents related to a given case in an individual health record framework (e.g., wellbeing screens, medical clinics, specialists). Having the capacity to scan documents supplied by numerous business representatives is thus essential for corporate employees.

To solve the issue of many watchwords in the different information owner's model, a search for multiple catchphrases (PRMSM) has been proposed as a solution. In spite of this, PRMSM wastes time and resources by compiling cypher texts from various sources for the same query. Using this method might be both costly and inefficient.

Because of this, it becomes more difficult to come up with a good approach for several clients. Each data owner's encrypted information is commonly organised into a tree-based list structure for the purpose of implementing security protection and responding to product inquires. Each data owner must establish a trap door for a given query condition, and the cloud must also search over each list to answer the question at hand. This method is obviously wasteful since the number of information owners is inversely proportionate to the number of trapdoors. Each data owner may have their records encrypted with a unique key, which simplifies the encryption process. Framework crashes are conceivable even if one of the owners is placed in peril.

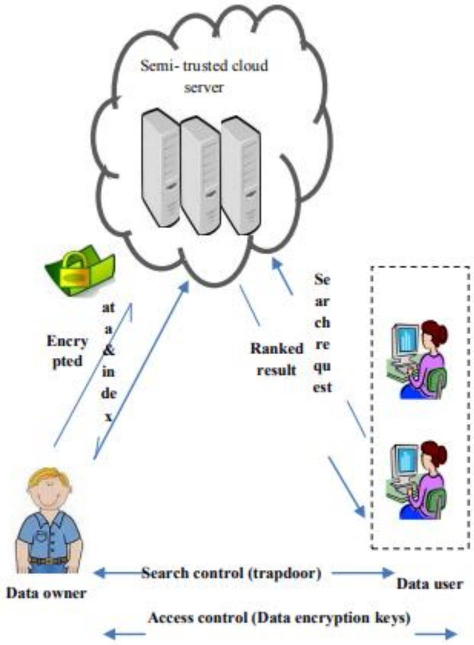
4. PROPOSED METHOD

A multi-source cloud architecture is being studied in which each source creates a tree-based file for his or her information documents and scrambles this information with a comparison key. Searching for many catchphrases in a single query using a tree-based search allows us to simultaneously conserve security while also increasing efficiency (TBMSM). These files may be merged into a single multi-watchword search on the cloud server without disclosing the information owners' private records or queries, as long as they are encoded.

By using bilinear mixing, we've developed a new approach to scrambling watchwords and trapdoors that may be used by information owners of diverse kinds of information. As a part of our "Depth-First Search" (DFS) algorithm, we use the TF IDF plan to rank the records according to their significance ratings. Final confirmation of our strategy's safety and efficacy comes through a complete hypothetical investigation and extensive data analysis..

This paper's summary includes the following pledges: It is possible for the cloud server to do an effective secure multi-watchword search without knowing the sensitive information of data owners since we give a unique search convention. This approach teaches users how to do different record trees so that they can answer queries more quickly. This technique enables each data owner to scramble their own tree-based record, and the cloud may successfully combine lists without knowing file content. The effectiveness of the TBMSM scheme is examined in detail using a real-world dataset, and the resulting logarithmic pursuit time is calculated.

SYSTEM ARCHITECTURE


Semi- trusted cloud server
Encry pted
at a & in de x
Ranked result
Se ar ch re qu est
Data owner
Search control (trapdoor)
Data user
Access control (Data encryption keys)

.

In an encrypted form, the owner of the data sends it to a cloud server from a number of different archival repositories. Information owners create a record collection quest tree file and encrypt the private report in the recommended strategy.. Encrypted data is sent to a cloud server, where it is decrypted by authorized information users, and then sent back to the cloud server. To access the owner's record, information clients must have permission from the latter party. When a customer has been accepted, he or she may enter search terms from the trapdoor and get encrypted files from the cloud.

The mystery key sent by the information owner enables the information client to decipher the information. Cloud servers hold the scrambled record and quest tree listings for the information owners. Upon receiving a query from the information client, the cloud server searches the file tree and delivers a list of the top-k encoding records. Many little pieces of protected cloud information look to the cloud server. It's used. The cloud server performs the query in accordance with the established protocol. As a result of the cloud server investigation, new data was gathered.

5. CONCLUSIONS AND FUTURE WORK

Different methods are used to record and examine the encoded material, for example. A multi-catchphrase search plot over encoded information is completed under a variety of information proprietor models that are evaluated for assessing the information involved in distributed computing. Every datum document's record tree is combined into a single tree. A DFS computation is used to do the searching. This is a safe hunt convention that allows different information owners to encrypt documents and records with separate keys. Because of the tree-based file structure for each datum owner, the cloud server may merge encoded lists with no prior knowledge of the data. As time goes on, this tree-based query plot becomes better at mapping watchwords than any other available approach.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] T. Peng, Y. Lin, X. Yao and W. Zhang, "An Efficient Ranked Multi-Keyword Search for Multiple Data Owners Over Encrypted Cloud Data," in IEEE Access, vol. 6, pp. 21924- 21933, 2018.

[2] Dawn Xiaoding Song, D. Wagner and A. Perrig, "Practical techniques for searches on encrypted data," Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000, Berkeley, CA, USA, 2000, pp. 44-55.'

[3] H. Yao, N. Xing, J. Zhou and Z. Xia, "Secure Index for Resource-Constraint Mobile Devices in Cloud Computing," in IEEE Access, vol. 4, pp. 9119-9128, 2016.

[4] P. Lu, S. Wu, L. Shou and K. Tan, "An efficient and compact indexing scheme for large-scale data store," 2013 IEEE 29th International Conference on Data Engineering (ICDE), Brisbane, QLD, 2013, pp. 326-337.

[5] Z. Shen, J. Shu and W. Xue, "Preferred keyword search over encrypted data in cloud computing," 2013 IEEE/ACM 21st International Symposium on Quality of Service (IWQoS), Montreal, QC, 2013, pp. 1-6.

[6] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen and W. Xie, "An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1265-1277, June 2016.

[7] M. S. Niaz and G. Saake, "Forward secure searchable symmetric encryption," 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Cambridge, 2017, pp. 49-54.